IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF:
ONE BLUE APPLE IPHONE OWNED BY
KHADIJAH ADAMS

Case No. 3:23-MJ-2012

Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Short, being first duly sworn under oath, state the following to be true to the best of my knowledge, information, and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since March 2019. I am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure. My primary duties and responsibilities involve the investigation of violations of federal law, including complex financial crimes as found in Title 18 United States Code, Sections 1341, 1343, 1344, 1349, and 1956. I am currently assigned to the Knoxville Field Office of the FBI and am assigned to the White Collar Squad. During my tenure as a Special Agent, I have investigated complex financial crimes including, but not limited to, frauds and swindles involving bank fraud, wire fraud, mail fraud, securities and commodities fraud, money laundering, and extortion. More specifically, I have conducted physical surveillance, assisted in the execution of search warrants, analyzed bank, phone, and internet records, and conducted arrests of criminal subjects. I have also spoken to confidential human sources, suspects, defendants, witnesses, and other experienced investigators concerning the methods and practices of the criminal element. I have gained experience through training at the FBI Academy, including training pertaining to interviewing and interrogation techniques,

arrest procedures, search and seizure, search warrant applications, and various other crimes and investigative techniques. I have had the opportunity to observe and review numerous investigations, in order to gain an understanding of the methods used by white collar criminals.

2. I am submitting this affidavit in support of an application for the issuance of a search warrant authorizing the examination an electronic device, a blue, Apple iPhone (hereinafter "Device") described in Attachment A, seized by law enforcement incident to arrest upon a federal complaint of Khadijah Adams (ADAMS) and owned by ADAMS, and the extraction from that property of electronically stored information described in Attachment B.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE TO BELIEVE ADAMS COMMITED WIRE AND MAIL FRAUD AND MONEY LAUNDERING

Background

5. The FBI is engaged in an investigation of subjects involved in schemes targeting a victim residing in the Eastern District of Tennessee and other victims elsewhere. The information in this affidavit is based on my personal knowledge and information. The facts set forth herein are based on my analysis of information from the victims, prior grand jury subpoenas, and prior search warrants in this investigation, which show that Khadijah Adams (ADAMS) with co-conspirators, Wigbert Bandie (BANDIE) and Mubarak Braimah (BRAIMAH), planned and orchestrated fraudulent financial transfers, via wire fraud and mail fraud, targeting unsuspecting victims. This

affidavit sets forth facts establishing probable cause to believe that ADAMS, utilized the Device in the acts of wire and mail fraud, and to launder money via "cash apps" and, that within the Device described in Attachment A, the items set forth in Attachment B currently exist, which constitutes evidence, instrumentalities, and/or fruits of the violations. This affidavit is not intended to include each and every fact related to this investigation, but only those facts necessary to support probable cause.

THE INVESTIGATION

The Fraud Scheme

6. This investigation was prompted by a complaint from a Knoxville, Tennessee, resident named Richard Coleman (COLEMAN), date of birth March 12, 1948, of a series of fraudulent financial transfers surrounding an investment scam, through which COLEMAN invested approximately $267,000 between July 2019 and October 2019.

7. In May of 2019, COLEMAN, recently widowed and looking for a relationship, was contacted by a person claiming to be "Kimberly Aaroon Mcintosh" (MCINTOSH), also claiming to be looking for a relationship, via Facebook messenger. MCINTOSH suggested moving conversation to Google Hangouts for privacy, and then they began exchanging text messages through COLEMAN's mobile carrier. Throughout this time, MCINTOSH emailed with COLEMAN using loveperfect083@gmail.com, and used the phone number 985-863-4375. MCINTOSH offered to give COLEMAN a 40% share of an inheritance of 189 kilograms of gold held in Singapore, and COLEMAN received a contract from MCINTOSH dated June 24, 2019.

8. COLEMAN was told for consideration of receiving the 40% share of the gold bars he would be paying fees for different parts of the process of shipping the gold to the United States. MCINTOSH put COLEMAN in contact with multiple people that were part of the operation. The

main individual facilitating COLEMAN's payment amounts and details was John Bothof (BOTHOF). BOTHOF's phone number was 208-425-6398, and his email was jbothof2019@aol.com. COLEMAN's understanding was that BOTHOF acted as a liaison and/or negotiator between COLEMAN and the company "Safety Shippers" whose URL was https://safetyshippers.co and email address was info@safetyshippers.co. Safety Shippers was allegedly the company responsible for shipping the gold to the United States. COLEMAN received a contract dated June 24, 2019, from both MCINTOSH and BOTHOF. The contract stated that "Richard Coleman has agreed to lend Kimberly Aaroon McIntosh all the financial support in the shipment of the gold bars to the United States and complete previously discussed business." The contract also stated that "40% of the gold bars will be given to Richard Coleman as an exchange of the money invested in the shipment."

9. COLEMAN was instructed by MCINTOSH and BOTHOF, for the purposes of securing the gold, paying attorney's fees, and customs/shipping fees, to send money via cash and cashier's checks to individuals specified by MCINTOSH and BOTHOF. One of those individuals was ADAMS. For example, some fees were to release the gold from Mexican customs for delivery to John F. Kennedy International (JFK) airport.

10. From July of 2019 through October 2019, in over ten to fifteen occasions, COLEMAN calculated having mailed cash to ADAMS at 110 East Henry Street, Apt. 1, Linden, NJ 07036. On two occasions, COLEMAN drew cashier's checks on his Knoxville TVA Employees Credit Union account and made two (2) electronic fund transfers (EFT) from his checking account to ADAMS's Bank of America (BOA) checking account X8458, claiming these funds were for shipping, import, and customs fees as indicated in the chart below:

Date	Description	Amount
7/12/2019	EFT via Counter Deposit to ADAMS BOA Account	$8,650.00
7/15/2019	EFT via Counter Deposit to ADAMS BOA Account	$10,000.00

11. In addition, COLEMAN sent cash money to ADAMS to her Linden, New Jersey address via the United States Postal Service (USPS) claiming these funds were for shipping, import, and customs fees as indicated in the chart below:

Date	Description	Amount
7/25/2019	Cash sent via USPS to/signed for by ADAMS	$25,000.00
8/7/2019	Cash sent via USPS to/signed for by ADAMS	$30,000.00

12. COLEMAN estimated that the total amount of money he sent to ADAMS, including EFTs and via the mail, was $267,000.

13. When COLEMAN eventually refused to provide more money, BOTHOF pressured COLEMAN to apply for loans or ask friends for money. BOTHOF offered to send COLEMAN a sample of the gold to prove the legitimacy of the contract. Soon thereafter, COLEMAN received a small sliver/shaving of gold as a sample of the inheritance from Sheila Whiteford (WHITEFORD) in Everett, Washington, via priority mail. Per instructions by BOTHOF, COLEMAN had the sample tested for purity at a local jeweler and then mailed it back.

Second Victim in the Fraud Scheme

14. In 2019, Helen Maksymicz (MAKSYMICZ), date of birth December 19, 1941, a Little Falls, New York, resident, contacted the FBI Syracuse Resident Agency to report that she and a friend, George Clingen (CLINGEN), date of birth October 22, 1939, had collectively lost approximately $388,423.33 in a scheme in which they were promised $7 million in gold bars from Syria. On December 17, 2017, MAKSYMICZ was on Facebook. Facebook suggested she add James Bradford (BRADFORD) as a possible friend. She added him and then wrote him a message

on Facebook Messenger. BRADFORD requested that they move their conversation to Google Hangouts, in which BRADFORD utilized jamesbradford205@gmail.com.

15. BRADFORD told MAKSYMICZ that he was from Huntsville, Alabama, and his wife died of cancer. BRADFORD said he was serving in the United States Army in Syria. While serving in Syria, he adopted a 12-year-old Syrian child named David after BRADFORD witnessed the death of David's mother and father. BRADFORD said David was being cared for by a Mary Ellen Lawrence (LAWRENCE) of Gordonsville, Tennessee, while BRADFORD was overseas.

16. BRADFORD told MAKSYMICZ that while in Syria he had obtained $7 million in gold bars and he needed help shipping the gold bars to the United States. BRADFORD offered MAKSYMICZ a percentage of the value of the gold bars if she funded the shipping charges. MAKSYMICZ agreed. BRADFORD had MAKSYMICZ sending money to Safety Shippers, who would contact her via the email info@safetyshippers.co. Safety Shippers is the same company and email address used in the scheme against COLEMAN.

17. By January 2, 2018, MAKSYMICZ began wiring money to various individuals as directed by BRADFORD for the shipment of gold. MAKSYMICZ sent money in various forms, e.g., wires, checks, and cash, to numerous individuals; however, she namely wired money to ADAMS and mailed checks to others. Both COLEMAN and MAKSYMICZ were instructed to send cash money to ADAMS at her Linden, New Jersey, address. In addition, MAKSYMICZ purchased Apple products to include, iTunes gift cards, iPhones, iPads, headphones, and computers, and shipped them to ADAMS with the understanding that they would be sold and the proceeds put toward the remaining cost of the gold shipment.

18. MAKSYMICZ also sent money in various forms to WHITEFORD in Everett, Washington. COLEMAN was directed to send money to WHITEFORD located in Everett, Washington.

19. MAKSYMICZ approached her friend CLINGEN, also of Little Falls, New York, to help with the costs and ultimately see a large return on his investment. According to their calculation, between the two of them, they had sent $388,423.33 to the scheme.

Third Victim in the Fraud Scheme

20. Sheila Faye Whiteford (WHITEFORD), date of birth July 11, 1942, of Everett, Washington, was interviewed. WHITEFORD met William Morrison[1] (MORRISON) on Facebook. The two of them continued communication through Google Hangouts. Morrison claimed he was in the military and currently stationed in Stuttgart, Germany, after being evacuated from Afghanistan during the U.S. troop withdrawal. She was told a story about a gold discovery and that financial help was needed. Safety Shippers contacted her in order to organize the shipments just like COLEMAN and MAKSYMICZ.

21. WHITEFORD estimated that she lost approximately $90,000 to the scheme, the earliest transfer being on or about February, 2017. There were three separate loans of $20,000, $10,000, and $10,000. Each time she sent money; it was cash via mail. She recalled sending money to two different places; one was in Florida and the other was to ADAMS at her Linden, New Jersey, address. WHITEFORD also received money from others. She recalled receiving $60,000 in cash and also receiving deposits in her J.P. Morgan Chase checking account which was

[1] Records from Google Search Warrant Case No. 3:21-MJ-2085 for Google account jamesbradford205@gmail.com and others, revealed that the account was linked by cookies to email account wmorrison19571803@gmail.com. Cookies are small pieces of data stored on a user's computer by the web browser, essentially meaning that the same machine was used to log into those accounts.

subsequently closed. Each time she received money; she was told where to send it. Sometimes she was directed to send the money via mail and, other times, through bank transactions.

22. On one occasion, WHITEFORD was instructed to go to Best Buy and pick up computers that were previously purchased, and subsequently instructed to mail them to ADAM's Linden, New Jersey address.

Analysis of ADAMS' Financial Institution Records

23. An analysis of ADAMS' financial records revealed that, since May, 2015, ADAMS has had accounts with at least six different financial institutions. A summary of the activity within those accounts is as follows:

Description/Activity	**Count**	**Total**
Wells Fargo (5/13/2015 - 4/19/2018)		
Incoming		
Cash and Check Deposits	105	$358,304.53
Incoming Wire Transfers	11	$64,700.00
Incoming Money App Transfers	13	$3,774.05
Legitimate Income – Spectrum for Living (non-profit organization providing housing and clinical services for the developmentally disabled)	56	$42,841.21
Outgoing		
Cash Withdrawals	242	$256,934.45
Cash Withdrawals in Ghana	44	$6,006.85
Outgoing Wire Transfer to ADD Minerals	1	$35,000.00
Outgoing Wire Transfers to Haruna Tia Mubarik	3	$34,500.00
Outgoing Wire Transfers to Adam Razak Abdul	10	$31,500.00
Outgoing Wire Transfers to Braimah Ndego Mubarak	3	$21,000.00
Outgoing Wire Transfer to Wunpini Company Limited	1	$2,000.00
Outgoing Money App Transfers	37	$9,898.95
JP Morgan Chase Bank (2/8/2017 - 8/5/2019)		
Incoming		
Transfers from Sheila Whiteford	22	$133,600.00
Cash Deposits	98	$77,603.34
Check Deposits	7	$11,900.00
MoneyGram/Money Order/Western Union Deposits	7	$7,680.00

Description/Activity	Count	Total
Incoming Money App Transfers	63	$13,795.63
Legitimate Income – Spectrum for Living	26	$21,585.02
Outgoing		
Outgoing Money App Transfers	308	$91,767.56
Cash Withdrawals	151	$45,333.63
Outgoing Wire Transfers to Braimah Ndego Mubarak	13	$23,700.00
Outgoing Wire Transfers to Adam Razak Abdul	5	$22,615.00
Bank of America (1/9/2019 - 8/2/2019)		
Incoming		
Cash Deposits	11	$36,030.00
Incoming Money App Transfers	5	$4,317.00
Cashier's Checks from Richard Coleman	2	$18,650.00
Incoming Wire Transfers	2	$16,240.00
Legitimate Income – Jewish Association for Developmental Disabilities	7	$5,579.69
Outgoing		
Cash Withdrawals	19	$19,469.00
Outgoing Wire Transfers to Braimah Ndego Mubarak	6	$24,200.00
Outgoing Wire Transfers to Adam Razak Abdul	1	$6,900.00
Outgoing Money App Transfers	54	$6,013.65
Columbia Bank (7/10/2019 - 8/20/2019)		
Incoming		
Cash Deposits	8	$24,380.00
Outgoing		
Cash Withdrawals	3	$20,500.00
Outgoing Money App Transfers	27	$3,253.95
TD Bank (7/31/2019 - 9/15/2021)		
Incoming		
Cash Deposits	92	$141,615.00
Check Deposits	1	$12,000
Incoming Money App Transfers	138	$76,575.39
Legitimate Income – Jewish Association for Developmental Disabilities	24	$28,509.03
Unemployment Income – State of New Jersey	97	$43,725.00
SBA EIDL Credit	1	$9,000
Outgoing		
Cash Withdrawals	111	$38,559.50

Description/Activity	Count	Total
Outgoing Money App Transfers	435	$136,001.77
Outgoing Wire Transfers to Braimah Ndego Mubarak	5	$36,670.00
Digital Federal Credit Union (6/22/2021 – 10/4/2021)		
Incoming		
Cash Deposits	3	$6,850.00
Transfers from Outside Bank	2	$58,060.00
Outgoing		
Outgoing Money App Transfers	7	$4,952.94
Outgoing Wire Transfers to Bassit Hassan	2	$58,050.00

ADAMS' Involvement in the Fraud Scheme;

24. A search warrant executed on ADAMS' Apple iCloud account khadijahseidu275@yahoo.com, revealed a series of exchanged text messages that had been backed-up to the iCloud. A verbatim conversation between ADAMS and BRAIMAH, from December 13, 2019 through December 14, 2019, read as follows:

BRAIMAH: "EL575898753US"[2]

BRAIMAH: "U awake"

BRAIMAH: "?????"

BRAIMAH: "What's up"

BRAIMAH: "Sleeping V"

BRAIMAH: "?"

ADAMS: "Yes I just woke up"

BRAIMAH: "Okay"

BRAIMAH: "Can you send me $500 through money gram when you get the pkg then you take it out ?pls ok"

ADAMS: "U skinny for too much now"

ADAMS: "Asking *"

BRAIMAH: "Lol"

[2] Note that this string of letters and numbers is a USPS tracking number.

ADAMS: "I ain't doing that"

BRAIMAH: "See you"

BRAIMAH: "Plz so I can get it here before the day ends here"

BRAIMAH: "Unless Monday"

BRAIMAH: "You get me?"

BRAIMAH: "You asleep again?"

ADAMS: "Am getting ready to leave the house . I have work this afternoon"

BRAIMAH: "Ok .so will you do my thing pls?"

ADAMS: "I can't"

BRAIMAH: "Did you track the usps pkg I sent you?"

ADAMS: "Am bout to track it rn"

BRAIMAH: "It's out for delivery"

BRAIMAH: "I just tracked it"

BRAIMAH: "Let me know when you get it ok"

ADAMS: "Okay am bout leaving the house tho . Nobody home"

BRAIMAH: "So call them and let's see if you can meet them or whatever"

ADAMS: "How much is it ?"

BRAIMAH: "There's $11,500 in the pkg."

ADAMS: "Okay"

ADAMS: "Okay I'll wait for it but I ain't taking 15% . So lemme know if u still want me receive it or u wanna send it to someone else ."

BRAIMAH: "What ?"

BRAIMAH: "I can't believe you are asking for 20%"

BRAIMAH: "So what is the difference between you and the other dudes?"

BRAIMAH: "??????"

ADAMS: "Yes . And I can't believe u tell ppl I take 20% and end up giving me 15% . And keeping the 5% that's very selfish .. and o even fly with this monies and all of that for 15% . No more . And u always talking honesty. Are u being honesty with me too. Big NO"

BRAIMAH: "Which people ?"

ADAMS: "U think u the only one that knows stuffs right . I'll just stay back and let u know it all"

ADAMS: "Just let me know if u still want me to take the package"

BRAIMAH: "Ok hold on"

ADAMS: "Or u wanna send it to someone else"

BRAIMAH: "Let me ask someone right now too So you know what % I give them"

BRAIMAH: "OBJ:OBJ"

BRAIMAH: "AND FOR YOUR POINT OF CORRECTION I DONT TAKE PEOPLES MONEY FOR THEM IF ITS NOT FROM MY JOB."

BRAIMAH: "Anyone who TOLD YOU I PICKED MONEY FOR THEM AND TOOK 20% We can ask that person or people"

BRAIMAH: "The monies you have been receiving are from jobs I control."

BRAIMAH: "Oh so now times that I gave you money more than the 15% you supposed to get never was a problem right ?"

BRAIMAH: "OBJ:OBJ"

BRAIMAH: "Look at the dates on the chats."

ADAMS: "The delivery guy is here"

ADAMS: "Should I take the package or not I need to know"

BRAIMAH: "I'm disappointed in you for telling me that"

BRAIMAH: "You can leave it Khadijah"

BRAIMAH: "I have never used someone's pal to send you money"

BRAIMAH: "Except my jobs I control which won't put you into trouble"

ADAMS: "And am very disappointed in u too"

BRAIMAH: "Any other persons money I use other people's account I don't use you ."

BRAIMAH: "Go believe whatever you want to.how long now have you been receiving money for me and it's always the same names for long.if I were taking for people it would have been different names all the time .so get your facts straight"

BRAIMAH: "So whoever you have that is feeding you with such info and you believe them Go ahead."

BRAIMAH: "I will still give you 15% and gift you with stuffs worth thousands of $$ and you can still ask for more?Thank you for bringing this up.i didn't know those were your thoughts now I know how you think and who you think like.👍"

ADAMS: "Don't gift me nothing no more and let me know if u want all ur gifts back . You've been these things against and talking all kind of shit to me . Who does that ., even to the extend of telling my frnd that if not because of u I wouldn't be whom I am rn... smh"

BRAIMAH: "And pls if you can let us ask the person who said i said you tKe 20% it would be the best to clear so I ask the person myself so you hear s"

BRAIMAH: "Go ahead and believe your friend 👍"

BRAIMAH: "I have people who I use to pick others money"

BRAIMAH: "If it's not my jobs I will never give your address to someone's job"

BRAIMAH: "So whoever said I said that I am still standing on it the person is a liar or the person should prove"

ADAMS: "Don't u handle other ppl job for them .,? You say I take 20% ., and it ain't even that . And even with this 15% it was a problem . First u just give whatever."

ADAMS: "We both don't need to talk to much"

ADAMS: "U know what u know and I know what I know"

BRAIMAH: "Besides sheila and Richard when last did someone else send you a pkg for me?"

BRAIMAH: "And Helen"

BRAIMAH: "Besides these 3[3] mention others you have received money from them on my behalf for the last 2 years ????"

BRAIMAH: "When you join my haters league and they are talking about me know the facts right before you come asking me.its obvious whoever told you this is a hater of mine,you can take that or leave that"

BRAIMAH: "These 3 are my jobs so go ahead and tell me the names of the other Peoples job I told them you take 20%"

25. The aforementioned Apple iCloud search warrant also revealed WhatsApp audio messages exchanged that were backed-up into the iCloud. Multiple undated audio messages are summarized as follows:

a. To a phone number likely controlled by an individual known as Kingsley Asong (ASONG), ADAMS stated that it would be very suspicious if ASONG deposited the "$26,000" and wired it on the same day. ADAMS advised that what she prefers to do is use money already in one account to send a wire and then use a separate account for deposit. ADAMS stated that the amount was too big to send to BRAIMAH, so instead she wanted ASONG to wire her $26,000, which she will subsequently send to "the guys."

[3] Note that the three names mentioned, Sheila, Richard, and Helen, are the three victims described in this affidavit.

b. In another message to ASONG, ADAMS told him that she has a package being delivered that day that contains $3,500 in cash under the name Annabella Smith. She asked him to pick up the package and she would send a calculated amount that he is to send to BRAIMAH.

c. From a phone number controlled by BRAIMAH, BRAIMAH told ADAMS to call a phone number from a missed call that also left a voicemail. The caller's name is James, and ADAMS was to portray an individual named Caroline who just arrived in Ghana and had to make a police report about lost bags and identification cards. She was to tell him that she was calling from a friend's phone number and for him to only contact that number going forward. BRAIMAH told ADAMS to just talk normal to James, as he was very sick, and to ask him about the hospital, whether he had seen the doctor, and to ask him about his legs.

d. In multiple messages to BRAIMAH, ADAMS asked for details on the scenario that she was to portray, what to say if certain questions were asked and, additionally, to report back on conversations had with multiple people.

26. The aforementioned Apple iCloud search warrant further revealed Safari browsing history that was backed-up into the iCloud. From June 12, 2021 through July 12, 2021, ADAMS' browser activity included the following:

a. A Facebook account creation URL;

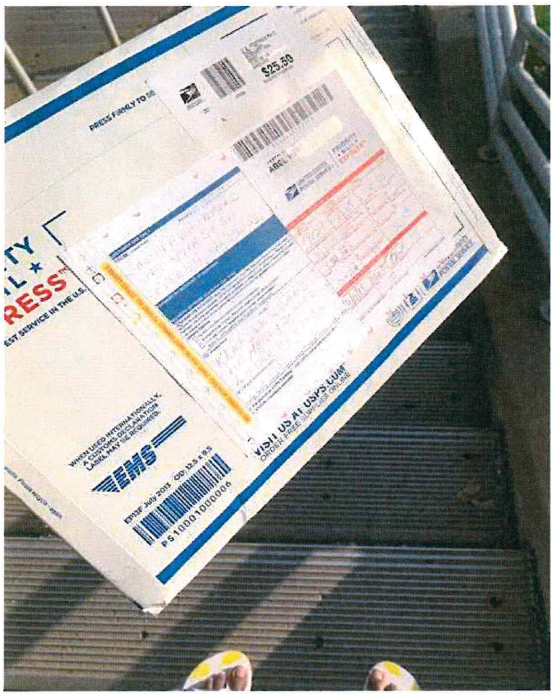
b. A Google account creation URL for jamesburger248@gmail.com;

c. An email received by the above Google account from Facebook to confirm the Facebook account creation;

d. A Google search of "can you make a 12000 check deposit with Td on mobile banking"; and

e. A login to chinalove.com utilizing the above Google account.

27. Additionally, as shown below, the aforementioned Apple iCloud search warrant revealed camera roll photographs of large cash bundles. Further, the camera roll contained photographic evidence of ADAMS' role in the scheme and her involvement in mail fraud, specifically by accepting a package sent from Sheila Whiteford, one of the victims described above.



ADAMS' ARREST

28. On November 28, 2022, I learned that ADAMS had purchased an airline ticket for an international flight departing from New York's JFK Airport to Ghana on November 30, 2022.

29. Based upon evidence obtained during the investigation, on November 29, 2022, I applied for an arrest warrant which was issued by the Honorable Jill E. McCook, United States Magistrate Judge.

30. The following day, on November 30, 2022, I, along with other members of the FBI, arrested ADAMS at JFK Airport, pursuant to the warrant. During the arrest, I seized a blue Apple iPhone that ADAMS held in her hand.

31. The Device is currently in storage at the FBI Knoxville Division field office, address 1501 Dowell Springs Blvd., Knoxville, Tennessee 37909. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

PROBABLE CAUSE TO BELIEVE iPHONE BELONGS TO ADAMS

32. Results of a July, 2021, search warrant on ADAMS' Apple ID khadijahseidu275@yahoo.com, DSID 386709903, revealed multiple means of utilizing the account and affiliated devices in the scheme, including a blue Apple iPhone. For example, text messages through iMessage and WhatsApp, audio messages through WhatsApp, and photos as described above were recovered.

33. In addition, the above account was owned and controlled by ADAMS, with an address of 110 E Henry St. Apt. 1, Linden, New Jersey, and a phone number 908-357-0855. A

federal grand jury subpoena to T-Mobile confirmed the number was held by Khadija Seidu,[4] date of birth 3/5/1996, from May 2021 to present day.

34. Text messages for the account spanned for years, from July 2017 to July 2021. Conversations recovered, like the one discussed above, included the percentage kept by ADAMS in the scheme and which jobs were controlled by BRAIMAH.

35. A federal grand jury subpoena to Apple confirmed the number was affiliated with the same aforementioned Apple ID and DSID for ADAMS, with the same address, and listed the device associated with the account as a blue iPhone. As stated above, the Device confiscated from ADAMS during her arrest was a blue iPhone.

36. Based on my training and experience, individuals that conspire to and commit mail and wire fraud schemes often use phones to that end. They further launder ill-gotten proceeds, especially via "cash apps," or phone applications, to make EFTs. And as discussed above, because fraud conspiracies typically rely upon electronic communications, such as voice calls, text messages, social media, it is reasonable to conclude that such evidence would be discovered on ADAMS' Device. Participants in fraud schemes such as this one, often take photographs of evidence of illegal activity to demonstrate to other fraudsters that they are "doing their part" to keep the fraud scheme going.

37. Further, because during the time period from the original iCloud search warrant to arrest, multiple financial institution records indicate continued activity consistent with continuation of the scheme, it is reasonable to conclude that the device confiscated during the arrest will contain further evidence of the scheme up to the day of the arrest.

[4] SEIDU was ADAMS's name prior to a legal name change upon ADAMS' United States naturalization.

38. As discovered from the search warrant executed on ADAMS' iCloud account, ADAMS' Apple iPhone phone should contain, *inter alia*, electronic correspondence such as email and text messages between ADAMS' co-conspirators, known and unknown to her, planning and executing the fraud scheme, messages arranging wire transfers, mail deliveries, and photographs of illegal activity and evidence of crimes.

TECHNICAL TERMS

39. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by

connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

40. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at www.apple.com/iphone, I know that the devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, evidence of a crime, or point toward the existence of evidence in other locations. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

41. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

42. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

h. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

i. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

j. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

k. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

l. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

m. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of

how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

44. *Method of retrieving evidence.* The nature of cellular phone-related evidence requires forensic analysts to employ a variety of different techniques to search for, document, and obtain electronic evidence. The search procedure may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

n. examination of all of the data contained in the cellular telephone, and/or memory storage devices in the cellular telephone to view the data and determine whether that data falls within the items to be seized as set forth herein;

o. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

p. surveying various file directories and the individual files they contain;

q. opening files in order to determine their contents;

r. scanning storage areas; and

s. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear.

45. *Manner of execution.* Because this warrant seeks only permission to examine a Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

46. Based on the foregoing information, there is probable cause to believe that ADAMS was a witting and complicit participant to the scheme to commit mail fraud, wire fraud, and launder money from February 1, 2017 to November 30, 2022. I request that the Court issue the proposed search warrant of the Device owned by ADAMS, incident to arrest on November 30, 2022, and currently in the possession of the FBI, as there is probable cause to believe that an examination of the Device described in Attachment A to seek the items described in Attachment B, will result in the collection of evidence relevant to an ongoing criminal investigation into the aforementioned criminal offenses.

Matthew Short
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 23rd day of January, 2023:

Honorable Jill E. McCook
United States Magistrate Judge
Eastern District of Tennessee